UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/083,448 | 02/25/2002 | Charles E. Perkins | 50072.0027USU1 | 6051 |

38879 7590 01/17/2006

DARBY & DARBY P.C.
P.O. BOX 5257
NEW YORK, NY 10150-6257

| EXAMINER | |
|---|---|
| NALVEN, ANDREW L | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 01/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/083,448 | PERKINS ET AL. | |
| | Examiner | Art Unit | |
| | Andrew L. Nalven | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *02.25/2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5 and 10-13* is/are rejected.

7)☒ Claim(s) *3,6-9 and 14-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. 8/19/05
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-19 have been examined.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1, 2, 4, 5, 10-13 and 19 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Lupien (US 6,463,055) in view of Marcovici et al. ("Global Authentication," Lucent Technologies TIA TR-56 Committee white paper, November 1999), hereafter Marcovici.

**Regarding claim 1**, Lupien discloses a method for strong authentication comprising:

sending a random number to a mobile node (random number RAND generated and sent to mobile station; col. 10, lines 46-52);

generating a MN signature using the MN, wherein the MN signature is generated using the random number (signature SRES generated using the random number RAND; col. 11, lines 8-10);

authenticating the MN to a network, wherein the network is a GPRS network (GPRS/GSM network; col. 10, lines 56-57; authenticating mobile station to the network by sending SRES in an "authentication response" message; col. 11, lines 1-10).

But Lupien does not explicitly explain (1) that the random number is generated local to the MN in a GPRS network and (2) authenticating the network to the MN.

However, Lupien teaches a GPRS network that integrates features of the ANSI-41 network (col. 3, lines 2-28), including integrating particular steps of authenticating a mobile station per ANSI-41 protocol with the GPRS authentication protocol for the purpose of efficiently providing GPRS services on an ANSI-41 network (col. 2, lines 57-63; col. 13, lines 7-24). Lupien also teaches that a step of ANSI-41 authentication includes generating a random number locally to the MN and transmitting it to the MN (RAND generated locally and sent to mobile station; col. 7, line 26) for the purpose of providing the mobile station with a random number for computing an authenticating signature (col. 7, lines 24-25). One of ordinary skill in the art would recognize that the random number RAND used to generate the ANSI-41 authenticating signature would be utilized as well to generate the GPRS authenticating signature, as this most closely parallels the legacy infrastructure as well as being a simple and secure means of generating a unique signature.

In addition, Marcovici teaches a method for strong authentication including the step of authenticating the network to the mobile station (page 5, section 4.1.1, particularly step e) for the purpose of enhancing the security of both ANSI-41 and GSM/GPRS authentication protocols (page 1, section 1).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lupien with the teaching of Marcovici to provide that the random number is generated local to the MN in a GPRS network and for authenticating the network to the MN. One would be motivated to do so in order to enhance security and provide GPRS services over an ANSI-41 network infrastructure.

**Regarding claim 2**, the modified method of Lupien and Marcovici is relied upon as applied to claim 1, and Lupien and Marcovici further teach that authenticating the MN to the network further comprises sending the MN signature to an authentication server; and verifying, by the authentication server, the mobile node signature (SRES sent to MSC/VLR or SGSN for verification; col. 11, lines 8-10). Therefore, for reasons applied above, such a claim also would have been obvious.

**Regarding claim 4**, the modified method of Lupien and Marcovici is relied upon as applied to claim 1, and Lupien and Marcovici further teach that authenticating the network to the MN further comprises generating an authentication signature by the authentication server and sending the authentication signature to the MN (Network Signature AS is generated and sent to mobile station; page 5, section 4.1.1, particularly step e). Therefore, for reasons applied above, such a claim also would have been obvious.

**Regarding claim 5**, the modified method of Lupien and Marcovici is relied upon as applied to claim 1, and Lupien and Marcovici further teach that the method of claim 4 further comprises verifying, by the MN, the authentication signature (Network Signature

AS is validated by mobile station; page 5, section 4.1.1, particularly step e). Therefore, for reasons applied above, such a claim also would have been obvious.

**Regarding claims 10-13 and 19**, these are system versions of the claimed method above (claims 1, 2, 4 and 5). Therefore, for the reasons applied above, such claims also would have been obvious.

***Allowable Subject Matter***

3. **Claims 3, 6-9 and 14-18 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

4. The following is a statement of reasons for the indication of allowable subject matter:

**Regarding claim 3**, the closest prior art, the modified method of Lupien and Marcovici, does not explain that the random number is generated by a base station. Lupien and Marcovici teach that the random number is "generated locally at the MSC level" but provide no suggestion that the base station generates the number (Lupien: col. 7, line 26). In fact, Lupien and Marcovici teach that for GPRS authentication the base station "acts as a transport only, except for air interface ciphering" (Lupien: col. 11, lines 22-23). As such, it would not seem obvious to one of ordinary skill in the art to modify the method of Lupien and Marcovici to provide that the random number is generated by a base station.

**Regarding claim 6**, the closest prior art, the modified method of Lupien and Marcovici, does not explain that the authentication server is a home authentication server (AAAH). Lupien and Marcovici teach that the authentication server is the MSC/VLR or SGSN and make no reference to a home authentication server (AAAH) or the authentication, authorization, and accounting (AAA) protocol.

Akhtar et al. (US 6,769,000) teaches use of the authentication, authorization, and accounting (AAA) protocol with conventional networks like GSM (col. 25, line 25-col. 26, line 59). But Akhtar et al. states that "strong authentication is preferred in the present invention" without providing motivation or sufficient detail pertaining the method of strong authentication to combine its teaching with Lupien and Marcovici, much less explaining how the AAAH would be integrated.

Therefore, it would not seem obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lupien and Marcovici to provide that the authentication server is a home authentication server (AAAH).

**Claims 7-9** are allowable by virtue of their dependence on claim 6.

**Regarding claims 14-18**, this is a system version of the claimed method above (claims 6-9). Therefore, for the reasons applied above, such claims also would be allowable.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

David Y. Jung
Primary Examiner

12/23/08